



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,242	06/26/2001	Zheng Qi	1875.9090002	3440

26111 7590 08/22/2006

STERNE, KESSLER, GOLDSTEIN & FOX PLLC  
1100 NEW YORK AVENUE, N.W.  
WASHINGTON, DC 20005

EXAMINER

PICH, PONNOREAY

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 08/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/892,242	<b>Applicant(s)</b> QI ET AL.	
	<b>Examiner</b> Ponnoreay Pich	<b>Art Unit</b> 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 08 August 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1,3-8,13-19,21,23,25-34,36 and 38-44 is/are pending in the application.
- 4a) Of the above claim(s) 44 is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1, 5-8, 13-19, 21, 23, 27-34, 36, 38, and 41-42 is/are allowed.
- 6) ☒ Claim(s) 3,4,25,26,39,40 and 43 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                                                                           |                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                                               | 4) <input checked="" type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. <u>8/2006</u> . |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                                      | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)                                  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>8/2006</u> | 6) <input type="checkbox"/> Other: _____                                                                     |

### **DETAILED ACTION**

This action is in response to amendments filed on 5/30/2006 and IDS filed on 8/8/2006. Applicant's amendments and arguments were fully considered, but are moot in view of new rejections presented below in response to the amended claims.

Applicant's amendment necessitated an election/restriction requirement due to newly added claims.

#### ***Election/Restrictions***

Restriction to one of the following inventions is required under 35 U.S.C. 121:

- I. Claims 1, 3-8, 13-19, 21, 23, 25-34, 36, and 38-43, drawn to an encryption apparatus, classified in class 380, subclass 37.
- II. Claim 44, drawn to an encryption method, classified in class 380, subclass 28.

The inventions are distinct, each from the other because of the following reasons:

Inventions II and I are related as process and apparatus for its practice. The inventions are distinct if it can be shown that either: (1) the process as claimed can be practiced by another and materially different apparatus or by hand, or (2) the apparatus as claimed can be used to practice another and materially different process. (MPEP § 806.05(e)). In this case the method can be performed by a materially different apparatus than invention I.

Art Unit: 2135

Because these inventions are independent or distinct for the reasons given above and have acquired a separate status in the art in view of their different classification, restriction for examination purposes as indicated is proper.

During a telephone conversation with Ms. Lori Gordon on 8/9/2006 a provisional election was made without traverse to prosecute the invention of group I, claims 1, 3-8, 13-19, 21, 23, 25-34, 36, and 38-43. Affirmation of this election must be made by applicant in replying to this Office action. Claim 44 is withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

***Information Disclosure Statement***

Documents listed in the IDS submitted by applicant on 8/8/2006 have been considered.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3, 4, 25, 26, 39-40, and 43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 3 defines the cryptography engine of claim 1 as a DES engine. The examiner notes that an engine of the data encryption standard has a well known structure. See further, Figure 12.2 on p272 of Schneier; Figure 3 of US 6,028,939; and Figure 6 of US 5,835,599 which disclose a standard DES engine. While one of ordinary skill would recognize that the majority of what is recited in claim 1 belongs to a DES engine, claim 1 also has the extra component of the "second circuitry configured to perform an exclusive OR (XOR) on the fourth bit sequence and a left portion of the input bit sequence for the current cryptographic round to generate a fifth bit sequence". This extra component means that the cryptography engine of claim 1 is an improvement upon a DES engine. As such, because of the improvement, one can no longer claim that the engine is a DES engine since DES is a standard. One cannot improve upon a standard and still say that what results is the same standard. Note that there is no XOR before the final permutation in a standard DES engine.
2. Claim 25 is indefinite for substantially the same reason as claim 3.
3. Claim 39 states that the cryptographic engine is configured to perform 3DES. Note that 3DES is performing DES three times. As discussed for claim 3, the cryptography engine of claim 1 is an improvement on a standard DES engine, thus the algorithm it performs is not DES since DES does not perform the second

XOR before the final permutation. As such, the engine also cannot be configured to perform 3DES since it does not perform DES. Claim 40 further defines claim 39 and use of DES operation by the engine. It too is rejected because DES is not performed by the improved engine, but rather an algorithm that is an improvement upon DES. An improvement upon a standard is not the same as the standard.

4. Claim 4 recites "an input bit sequence" in line 3, which should be "the input bit sequence" since "an input bit sequence" was earlier recited already. Claim 26 has a similar problem.
5. Claim 43 should recite in the last line: "... of the fourth size to the third size for further processing."

#### ***Allowable Subject Matter***

Claims 1, 5-8, 13-19, 21, 23, 27-34, 36, 38, and 41-42 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: As per claims 1 and 23, the majority of what is recited is found in a standard DES engine, i.e. the key scheduler, the expansion logic, the first circuitry, the substitution box, and the permutation logic. However, the prior art does not appear to teach the additional component of "a second circuitry configured to perform an exclusive OR (XOR) on the fourth bit sequence and a left portion of the input bit sequence for the

current cryptographic round to generate a fifth bit sequence", the second circuitry coupled to the final permutation logic.

Claims 3, 4, 25, 26, 39-40, and 43 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PP

Ponnoreay Pich  
Examiner  
Art Unit 2135



**KIM VU**  
**SENIOR ADVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**